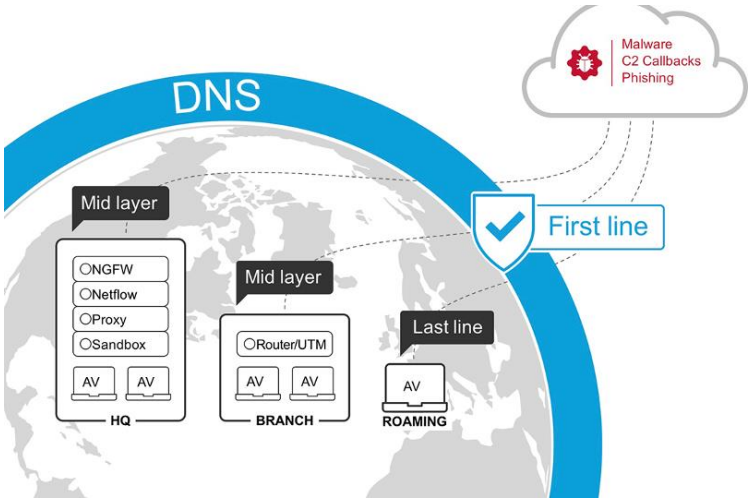
Cisco Umbrella – Effektiver Schutz gegen Ransomware

Nicht erst seit „WannaCry“ ist Ransomware ein ernsthaftes Problem für Unternehmen. Diese Art von Malware, welche Daten auf Computern verschlüsselt, nimmt immer mehr zu. Angreifer fordern Lösegeld von betroffenen Unternehmen für die Wiederherstellung der Daten – was oft genug nach erfolgter Zahlung ein leeres Versprechen bleibt. Ransomware entwickelte sich für Angreifer zur bisher profitabelsten Malware-Art. Es gibt viele Möglichkeiten, wie Ihre Systeme von Ransomware befallen werden können – Weblinks, Malvertising, Phishing-E-Mails und modifizierte USB-Sticks laden unbemerkt die Verschlüsselungssoftware aus dem Internet herunter und die verseuchten Systeme verbinden sich bei der Infektion zum ‚Command&Control-Server‘, um die Schlüssel auszutauschen. Hier bietet Cisco mit Umbrella einen frühzeitigen Schutz gegen das Herunterladen der Verschlüsselungsmalware durch Unterbindung der Kommunikation zum C&C-Server. Umbrella prüft bei der Auflösung von DNS-Adressen deren Reputation basierend auf Analysewerten des Traffic-Verhaltens sowie aufgrund von Informationen von ‚Cisco Talos‘, dem weltweit führenden ‚Threat Intelligence Team‘ von Cisco. Malware-Zugriffe auf Web-Seiten mit schlechter Reputation können so blockiert werden. Die meisten Ransomware-Angriffe können mit Umbrella bei der Kommunikation mit einem C&C-Server auf DNS-Layer gestoppt werden, bevor die Malware mit der Verschlüsselung der Daten beginnt. Der Schutz greift bei sämtlichen Zugriffen auf das Web durch PCs, Server, mobile Geräte sowie durch IOT-Geräte wie Kameras, Drucker usw.

Abb. 1: DNS erste Verteidigungslinie gegen Ransomware-Angriffe (Quelle: Cisco)



Vorteile auf einen Blick - Eine neue Schutzschicht in der Bedrohungsabwehr

+ Schutz vor Bedrohungen, erste Verteidigungslinie

+ Schutz, der auch ohne Anbindung an das Unternehmensnetzwerk greift

+ Immer auf dem aktuellen Stand - Geräte müssen für Updates nicht mittels VPN mit dem Unternehmen verbunden sein

+ Blockierung von Domains, IPs und URLs

+ Schlüsselfertige und kundenspezifische API-basierte Integrationen

Mehr Informationen zum Thema finden Sie unter folgendem Link oder durch Kontaktaufnahme via info@ispin.ch